UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

TREVOR SLOAN, JOSEPH BLEIBERG, ARYEH LOUIS ROTHBERGER, PATRICK COMMERFORD, KEVIN FARR, ELMER ORPILLA, and KEITH LAPATING, on behalf of themselves and all others similarly situated, Plaintiffs, v. ANKER INNOVATIONS LIMITED, FANTASIA TRADING LLC, and POWER MOBILE LIFE LLC, Defendants.	Case No.: 1:22-cv-07174 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**
SAGAR DESAI, individually and on behalf of all others similarly situated, Plaintiff, v. ANKER INNOVATIONS LIMITED, FANTASIA TRADING LLC, and POWER MOBILE LIFE LLC Defendants.	Case No.: 1:23-cv-01607

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs Trevor Sloan, Joseph Bleiberg, Aryeh Louis Rothberger, Patrick Commerford, Kevin Farr, Sagar Desai, Elmer Orpilla, and Keith Lapating (collectively, "Plaintiffs") bring this Consolidated Class Action Complaint against Defendants Anker Innovations Limited ("Anker Innovations"), Fantasia Trading LLC ("Fantasia,"), and Power Mobile Life LLC ("Power Mobile," and, together with Anker Innovations and Fantasia, "Anker"

or "Defendants"), individually and on behalf of all others similarly situated, and complain and allege upon personal knowledge as to themselves and their own acts and experiences and, as to all other matters, upon information and belief, including an investigation conducted by their attorneys, as follows:

NATURE OF THE ACTION

1. Anker manufactures, distributes and sells its "eufy" branded security products. As part of its "eufy" security offering, Anker sells home security cameras, including its eufycam, Video Smart Lock, SoloCam, Floodlight Cam, Video Doorbell, and Solo Indoorcam lines of products (collectively, the "Camera Products"). The Camera Products are equipped with Wi-Fi, and advertised to send signals that are encrypted and capable of recording video, streaming video, facial recognition, motion detection, and, notably, the ability to send notifications when the motion detection is triggered. This action seeks damages for Plaintiffs and other consumers who were victims of Defendants' fraudulent representations concerning the Camera Products' security and privacy features.

2. Anker's marketing for its Camera Products expressly touted that the products saved all video recordings and conducted all facial recognition *locally* (meaning on equipment located with and controlled by the consumer). In other words, Anker's marketing materials represented that only the end user had access to videos and images displayed, streamed and/or recorded by the Camera Products.

3. Anker used this and other claims to differentiate its Camera Products from competitors', which often require their similar cameras to access the internet to work. These touted design features were material to purchasers of the Camera Products, including Plaintiffs. Indeed, Anker's most direct competitor, "Nest," which is manufactured by Google,

requires all cameras to be connected to Nest servers, which record and process the data remotely, before sending it back to the user.

4. For example, Anker's marketing materials promised that "your recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you." In addition, Anker's marketing materials assured consumers that the Camera Products conduct facial recognition *locally*, rather than transmitting them to cloud storage.

5. These and other substantively similar statements by Anker were untrue.

6. In November 2022, security researcher Paul Moore ("Moore") revealed that eufy cameras upload images and facial recognition data to Defendants' cloud storage, which is hosted by a third party (Amazon Web Services ("AWS"), a subsidiary of Amazon.com, Inc.), even where the user did not sign up for cloud storage or services. Moore also found that a separate Camera Product linked to a different account was able to identify his face with the same unique ID — which meant that Anker was not only storing facial recognition data in the cloud, but also sharing that back-end information between accounts.

7. Moore also noted that he was able to view live footage from his camera over a web browser without any kind of authentication; he simply navigated to the correct public-facing web address and viewed the footage. This meant that the Camera Products were not made with end-to-end encryption, and thus Anker's security marketing statements were patently false and misleading.

8. Defendants eventually conceded that, even for users who did not create a cloud account or agree to the transmittal of images from their eufy camera to Defendants' cloud

storage, such images were nevertheless collected, transmitted, and disseminated to the third-party company that hosts Defendants' cloud storage for consumers.

9. Defendants claimed that it was an "oversight" and an "error" to have represented that they did not engage in this practice and promised to change their marketing and other consumer-facing materials to make this clear. As of December 20, 2022, however, Defendants continued to falsely advertise the Camera Products as operating with "No Clouds" and make other misleading claims concerning their security products. Defendants eventually came clean at the end of January 2023, but insisted that, while its Camera Products previously had not had end-to-end encryption and did not store all data locally, the security defects had been fixed.

10. Plaintiffs and consumers viewed Anker's false and misleading marketing prior to their purchases and reasonably relied on Anker's marketing when purchasing the Camera Products. Plaintiffs and other members of the Class, however, did not receive the products that they were promised, *i.e.*, security cameras that did not share their data with any third parties, including Anker, and that were secured by end-to-end encryption. Additionally, Plaintiffs and other members of the Class have had their biometric information uploaded to Anker's servers without their authorization. Accordingly, Plaintiffs bring this class action on behalf of: (i) all individuals in the United States who purchased Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period (the "Nationwide Class"); (ii) all individuals in the State of Illinois who purchased Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period (the "Illinois Class"); (iii) all individuals in New York State who purchased Camera Products for personal or household use, and not for resale, during the applicable

statute of limitations period (the "New York Class"); (iv) all individuals in the Commonwealth of Massachusetts who purchased Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period (the "Massachusetts Class"); and (v) all individuals in the State of Florida who purchased Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period (the "Florida Class"), to recover restitution and damages, and for injunctive relief.

PARTIES

11. Plaintiff Trevor Sloan ("Sloan") is a resident and citizen of Illinois who purchased and used a eufy branded Video Doorbell and Floodlight Camera. Sloan purchased these Camera Products in 2021, from Best Buy. Sloan also downloaded and installed Defendants' eufy Security app for use with these Camera Products. Sloan purchased these Camera Products, in part, because they purportedly stored all information locally and did not upload information to Anker's servers. Prior to purchase, Sloan read and relied on Anker's representations concerning the security and privacy of the Video Doorbell and Floodlight Camera, including the labeling representations that "Your Privacy is something that we value as much as you do. To start, we're taking every step imaginable to ensure that your data remains private, with you. Whether it's your newborn crying for mom, or your victory dance after a game, your recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you." Sloan also read and relied on Anker's representations that "[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you" and the Camera Products have "Military-Grade AES-256 data encryption." Furthermore, images of Sloan and others were captured by the Camera Products and thereafter transmitted and disseminated to Defendants' cloud storage hosted by

a third party and subjected to facial recognition technology, which generated a face template or faceprint of individuals captured in such images. Had Sloan known the Camera Products captured biometric data and uploaded pictures and video online to Anker's servers, with minimal security, or that his pictures and video were not encrypted or could be accessed by unknown third-parties, he would not have purchased the Camera Products or would have paid less.

12. Plaintiff Joseph Bleiberg ("Bleiberg") is a resident of Queens, New York. In or about November 2020, Bleiberg purchased a eufy Wireless Video Doorbell in Queens, New York. Since then, Plaintiff has used his eufy camera at his home in Queens, New York. Bleiberg also downloaded and installed Defendants' eufy Security app for use with his eufy camera. Bleiberg chose to purchase a eufy camera, rather than competing products, because he read and relied on Defendants' representations concerning the security and privacy features of eufy cameras, including their claims that eufy cameras operated with "no cloud," that only the user had access to images captured by the camera, and that eufy cameras used strong encryption. Images of Bleiberg and members of Bleiberg's family and visitors to Bleiberg's home were captured by the eufy camera and thereafter transmitted and disseminated to Defendants' cloud storage hosted by a third party and subjected to facial recognition technology, which generated a face template or faceprint of individuals captured in such images. When Bleiberg learned that his eufy camera shared images with Defendants' cloud, he tried to find a way to disable the cloud-sharing function. Had Bleiberg known the truth about Defendants' collection and dissemination of images captured by his eufy camera, or about Defendants' deficient privacy and security practices, he would not have purchased, or would have paid less for, his eufy camera.

13. Plaintiff Aryeh Louis Rothberger ("Rothberger") is a resident and citizen of Flushing, New York, who purchased and used a eufy security Video Doorbell Kit from Amazon.com on June 21, 2021, and purchased a eufy security wireless add-on from Amazon.com on December 10, 2021. Rothberger purchased these Camera Products, in part, because they purportedly stored all information locally and did not upload information to Anker's servers. Rothberger read and relied on Anker's representations concerning the security and privacy of the Video Doorbell, including the representations that "Your Privacy is something that we value as much as you do. To start, we're taking every step imaginable to ensure that your data remains private . . . . [Y]our recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you." Rothberger also read and relied on Anker's representations that "[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you" and the Camera Products have "Military-Grade AES-256 data encryption." Furthermore, images of Rothberger and others were captured by the Camera Products and thereafter transmitted and disseminated to Defendants' cloud storage hosted by a third party and subjected to facial recognition technology, which generated a face template or faceprint of individuals captured in such images. Had Rothberger known the Camera Products captured biometric data and uploaded pictures and video online to Anker's servers, with minimal security, or that his pictures and video were not encrypted or could be accessed by unknown third parties, he would not have purchased the Camera Products or would have paid less.

14. Plaintiff Sagar Desai ("Desai") is a Florida citizen residing in Miami-Dade County. On or about February 18, 2021, Desai purchased four (4) eufy Security eufyCam 2 wireless cameras from Amazon.com. On or about September 7, 2021, Desai and his family

purchased two (2) eufy Floodlight Cameras, one (1) eufy Video Doorbell 2K (Wired) and one (1) eufy Solo IndoorCam P24 (Wired) from Amazon.com. On or about October 6, 2021, Desai and his family purchased a eufy Security Solo OutdoorCam c24 from Amazon.com. On or about October 27, 2021, Desai and his family purchased a eufy Security Floodlight Camera from Amazon.com. On or about December 7, 2021, Desai and his family purchased a eufy Security Solo IndoorCam P24 camera from Amazon.com. On or about April 21, 2022, Desai and his family purchased two (2) eufy SoloCam L20 cameras directly from eufy's online store. On or about November 12, 2022, Desai and his family purchased one (1) eufy HomeBase 3, one (1) eufy Solar Panel Charger, one (1) eufy SoloCam S40, and one (1) eufy Entry Sensor directly from eufy's online store. Desai purchased these cameras after performing online research for a home security and home monitoring option that provided safe, secure, and private encrypted services. Desai read and relied on Anker's representations as to its privacy, and its privacy commitments as advertised on both Anker's eufy website and on its product pages at Amazon.com when buying the aforementioned eufy Camera Products. Desai set his eufy Security Cameras up both outside and inside his house to not only help him monitor his property but to also serve as "baby monitors" so that he could keep an eye on his young children. Desai proactively elected to not use Anker's cloud storage option, instead relying on his HomeBase and microsd cards that he provided himself and inserted into certain of his cameras to keep his camera's recordings "local" to his property. Desai did elect to utilize Anker's push notification system so that his cameras would send him notifications when they captured movement, or when his doorbell was activated. Desai, at all times, believed, as a result of Anker's representations both online and on the packaging of the products he purchased, that the images captured by his cameras would be solely stored locally,

would be encrypted, and would not be stored in Anker's cloud in any way. Desai relied on Anker's representations when he utilized the eufy Securities live view feature on its web-portal feature to view images from his family's cameras. Had Desai known his, his family's, and other people's images and biometric information would be captured and stored on the cloud by Anker or that his camera feeds were not encrypted or could be accessed by unknown third parties, he would not have purchased these Camera Products or would have paid less than he did.

15. Plaintiff Patrick Commerford ("Commerford") is a Texas citizen residing in Harris County, Texas. On or about June 29, 2020, Commerford purchased a eufy Security, Wi-Fi Video Doorbell, 2K Resolution from eufyHome through Amazon.com. On or about August 16, 2020, Commerford purchased two eufy Security Indoor Cam 2K Pan and Tilt cameras from Amazon.com. Commerford purchased these cameras after performing online research for a home security and home monitoring option that provided safe, secure, and private encrypted services. Commerford read and relied on Anker's representations as to its privacy, and its privacy commitments as advertised on both Anker's eufy website, on its product pages at Amazon.com when buying the aforementioned eufy Camera Products, and on the product packaging. Commerford set his eufy security cameras up both outside and inside his house to not only help him monitor his property but to also serve as "baby monitors" to keep an eye on his young children. Commerford proactively elected to not use Anker's cloud storage option, instead relying on his HomeBase and microsd cards that he provided himself and inserted into his cameras to keep his camera's recordings "local" to his property. Commerford did elect to utilize Anker's push notification system so that his cameras would send him notifications when they captured movement, or when his doorbell was activated.

Commerford, at all times, believed, as a result of Anker's representations both online and on the packaging of the products he purchased, that the images captured by his cameras would be solely stored locally, were encrypted, and would not be stored in Anker's cloud in any way. Commerford relied on Anker's representations when he utilized the eufy Securities live view feature on its web-portal feature to view images from his family's cameras. Had Commerford known his, his family's, and other people's images and biometric information would be captured and stored on the cloud by Anker or that his live camera feeds could be accessed by unknown third parties, or were not encrypted, he would not have purchased the eufy Security Cameras or would have paid less than he did.[1]

16. Plaintiff Kevin Farr ("Farr") is a Massachusetts citizen residing in Barnstable County, Massachusetts. On or about October 19, 2021, Farr purchased a eufy Security, solo IndoorCam P22, 1080p Indoor Camera from eufyHome through Amazon.com. Farr purchased this camera after performing online research for a home security and home monitoring option that provided safe, secure, and private encrypted services. Farr read and relied on Anker's representations as to its privacy and its privacy commitments as advertised on both Anker's eufy website, on its product pages at Amazon.com when buying the aforementioned eufy Camera Products, and on the product packaging. Farr set his eufy security camera up inside his house to not only help him monitor his property but to also serve as monitor for his family's pet dog. Farr proactively elected to *not* use Anker's cloud storage option, and instead choose to view the footage from his camera live, without it being recorded anywhere. Farr did elect to utilize Anker's push notification system so that his camera would send him

[1] On February 23, 2023, Commerford, by and through counsel, made a formal written demand via certified mail and email on Defendants Fantasia Trading, LLC, Power Mobile Life LLC, and Anker Innovations Limited, in accordance with Texas Business and Commerce Code Sections 17.50 and 17.505.

notifications when it captured movement. Farr, at all times, believed, as a result of Anker's representations both online and on the packaging of the products he purchased, that the images captured by his camera would not be stored in Anker's cloud in any way. Farr relied on Anker's representations when he utilized the eufy' Securities live view feature on its web-portal feature to view images from his family's camera. Had Farr known his, his family's, and other people's images and biometric information would be captured and stored on the cloud by Anker or that his live camera feeds would not be encrypted or could be accessed by unknown third parties, he would not have purchased his eufy Camera Product or would have paid less than he did.

17. Plaintiff Elmer Orpilla ("Orpilla") is a resident and citizen of the state of Illinois. Between September of 2020 and April of 2021, Orpilla purchased several Camera Products (two eufyCam 2C 1080p Wireless cameras, two eufyCam 2C Pro 2k Wireless cameras, a eufy 2k Indoor 2-Cam Kit, and Video Doorbell) from Amazon.com. When purchasing the Camera Products, Orpilla reviewed the accompanying labels and disclosures, and understood them as representations and warranties by Defendants that the products would store data locally and securely using military encryption. Orpilla relied on these representations and warranties in deciding to purchase the Camera Products and these representations and warranties were part of the basis of the bargain in that he would not have purchased the Camera Products if he had known what Defendants omitted: that they would transmit his data to cloud servers, allow for unencrypted access to his cameras, or send unencrypted transmissions with his information to the cloud. When Orpilla installed the

Camera Products as directed by Defendant, Orpilla utilized the thumbnail notification system. If Anker remedied these problems, Orpilla would purchase eufy products again.

18. Plaintiff Keith Lapating ("Lapating") is a resident and citizen of the state of California. On November 5, 2021, Lapating purchased one of the Camera Products (Video Doorbell 2k HD, Model TP8210) from Best Buy in California. When purchasing the Camera Products, Lapating reviewed the accompanying labels and disclosures, and understood them as representations and warranties by Defendants that the products would store data locally and securely using military encryption. Lapating relied on these representations and warranties in deciding to purchase the Camera Products and these representations and warranties were part of the basis of the bargain in that he would not have purchased the Camera Products if he had known what Defendants omitted: that they would transmit his data to cloud servers, allow for unencrypted access to his cameras, or send unencrypted transmissions with his information to the cloud. When Lapating installed the Camera Products as directed by Defendant, Lapating utilized the thumbnail notification system. If Anker remedied these problems, Lapating would purchase eufy products again.

19. Defendant Anker Innovations is a Hong Kong company with its principal place of business at Room 1318-19, Hollywood Plaza, 610 Nathan Road, Mongkok, Kowloon, Hong Kong SAR, People's Republic of China. Anker Innovations designs and manufactures Camera Products for export and sale throughout the world, including throughout the United States and in New York and Illinois. Anker Innovations offers the eufy Security App for use with eufy cameras, including by users in Illinois, New York, Massachusetts, Florida, and Texas.

20. Defendant Fantasia is a Delaware limited liability company headquartered in Ontario, California. Fantasia manufactures and markets various electronic devices and

accessories under its own brand, Anker, as well as other brand names including eufy, Soundcore, Nebula, and Roav.

21. Defendant Power Mobile, LLC is a Washington limited liability company with headquarters in Bellevue, Washington. Power Mobile Life, along with its co-Defendants, manufactures and markets the eufy Security Cameras at issue in this litigation.

22. Defendants Anker Innovations, Fantasia, and Power Mobile acted jointly to perpetrate the acts described herein, including the manufacture, labeling, marketing, and collection of biometric data relating to the Camera Products, and they are thus subject to joint and several liability. At all times relevant to the allegations in this matter, each Defendant acted in concert with, with the knowledge and approval of, and/or as the agent of the other Defendants within the course and scope of the agency, regarding the acts and omissions alleged.

23. Plaintiffs reserve the right to amend this complaint to add different or additional defendants, including without limitation any officer, director, employee, supplier, or distributor of Defendants and/or the Camera Products who has knowingly and willfully aided, abetted, or conspired in the false and deceptive conduct alleged herein.

JURISDICTION AND VENUE

24. This Court has subject matter jurisdiction over this class action under 28 U.S.C. § 1331 because this complaint asserts a claim arising under the laws of the United States. In addition, this Court has subject matter jurisdiction over this matter pursuant to 28 U.S.C. § 1332 of the Class Action Fairness Act of 2005 because: (1) there are 100 or more putative Class members, (ii) the aggregate amount in controversy exceeds $5,000,000.00, exclusive of interest and costs, and (iii) there is minimal diversity because Plaintiffs and Anker are citizens

of different states. This Court has supplemental jurisdiction over Plaintiffs' state law claims pursuant to 28 U.S.C. § 1367.

25. This Court has personal jurisdiction over Anker because it has substantial aggregate contacts with this District, including engaging in conduct in this District that has a direct, substantial, reasonably foreseeable, and intended effect of causing injury to persons throughout the United States, including by marketing and selling Camera Products to consumers in this Judicial District, by placing Camera Products into the stream of commerce directed at this Judicial District, and because Anker purposely availed itself of the laws of the United States and the State of Illinois. Furthermore, pursuant to the End User License Agreement for Camera Products (including the cameras purchased and used by Plaintiffs) and the eufy Security App (the "EULA"), Defendants irrevocably submitted to the jurisdiction of any federal or state court located in Cook County, Illinois, which is within this Judicial District.

26. In accordance with 28 U.S.C. § 1391, venue is proper in this District because the parties consented to jurisdiction of this Court, Anker transacts business in this District, and Anker has intentionally availed itself of the laws and markets within this District. Furthermore, venue is proper in this Judicial District pursuant to 28 U.S.C. § 1391(b) because the EULA provides that any claim, dispute, action, cause of action, issue, or request for relief relating to the EULA will be governed by the laws of Illinois, without giving effect to any conflicts of laws principles that require the application of the laws of a different jurisdiction, and that any action or proceeding relating to the EULA must be brought in a federal or state court located in Cook County, Illinois.

FACTUAL ALLEGATIONS

A. Background Information

27. Anker markets, distributes, and sells its "eufy" branded Camera Products throughout the United States. Consumers can purchase these Products online, either directly through Anker or another online retailer, or at brick-and-mortar store, such as Best Buy. These Camera Products are specifically marketed for home security, allowing consumers to view live and recorded video of the areas around their homes and to automatically receive notifications on their cell phone, tablet, or computer regarding activity detected by the cameras, including thumbnail images when a person is detected in the cameras' field of view or when a person presses the doorbell. Defendants' eufy branded security cameras include the eufyCam product line (such as the eufyCam 2, eufyCam 2 Pro, eufyCam 2C, eufyCam 2C Pro, and the S-3300 eufyCam (also known as the eufyCam 3)), the SoloCam product line (such as the SoloCam S40), and the Solo IndoorCam product line (such as the Solo IndoorCam C24). Some eufy cameras, such as the Video Doorbell Dual and other "doorbell cameras," also allow users to hear and speak to persons standing near the doorbell.

28. The Camera Products also have the BionicMind system, marketed as a "local artificial intelligence used for facial recognition." The BionicMind system enables eufy cameras to differentiate between known individuals and strangers by recognizing biometric identifiers (*i.e.*, details about the face's geometry as determined by facial points and contours) and comparing the resulting "face template" (or "faceprint") against the face templates stored in a database.

29. Consumers who purchase the Camera Products must use the eufy Security smartphone application (the "eufy Security App"). To set up the eufy Security App,

consumers provide their email address and other personally identifiable information. The eufy Security App allows users to access their cameras, view live and historical video feeds, and adjust the cameras' settings. The Camera Products communicate with the eufy Security App to provide user notifications, such as notification of activity on the cameras.

30. The End User License Agreement ("EULA") for the application and the Camera Products provides that "you agree that this EULA, and any claim, dispute, action, cause of action, issue, or request for relief relating to this EULA, will be governed by the laws of Illinois, without giving effect to any conflicts of laws principles that require the application of the laws of a different jurisdiction. Any action or proceeding relating to this EULA must be brought in a federal or state court located in Cook County, Illinois and each party irrevocably submits to the jurisdiction and venue of any such court in any such claim or dispute."

B. Anker's Privacy Marketing

31. At all relevant times, Defendants designed and conducted a long-term marketing campaign touting the supposed privacy and security features of the Camera Products. Defendants did so to target and appeal to privacy-conscious consumers and to distinguish the Camera Products from competing products. Defendants touted that only the user can access data associated with that user's Camera Products, that the data is stored locally and not sent to Defendants, and that the data is always encrypted. Accordingly, Anker touts that no one, other than the user, can access the data associated with the Camera Products.

32. Each of the Camera Products, on the Product's label, advertises and warrants that:

- "Your Privacy is something that we value as much as you do."

- "To start, we're taking every step imaginable to ensure that your data remains private, with you."
- "Whether it's your newborn crying for mom, or your victory dance after a game, your recorded footage will be kept private."
- "Stored locally. With military-grade encryption."
- "And transmitted to you, and only you."
- "That's just the start of our commitment to protect you, your family, and your privacy."

Additionally, the Camera Products' labels also advertise and warrant that "[a]ll your footage is securely stored locally[,] [e]nsuring the videos you record are for you and only you" and that the Products have "Military-Grade AES-256 data encryption." Anker's privacy marketing does not end here.

33. Indeed, during the relevant time period, Anker's website included a "Privacy Commitment," which states that "eufy Security, privacy and protection are our top priorities. Both are integral to our daily operations, and to implementing measures that ensure your data is always safe." Anker noted that all information would be stored locally and be encrypted so only the user could see it. Similarly, Anker promised that its AI would not send pictures to the cloud.

Anker continued, noting that video would never be shared with Anker or any third parties unless expressly authorized:

- "To start, we're taking every step imaginable to ensure your data remains private, with you."
- "[Y]our recorded footage will be kept private. Stored locally. With military-grade encryption. And transmitted to you, and only you."
- "With secure local storage, your private data never leaves the safety of your home, and is accessible by you alone."
- "There is no online link available to any video."

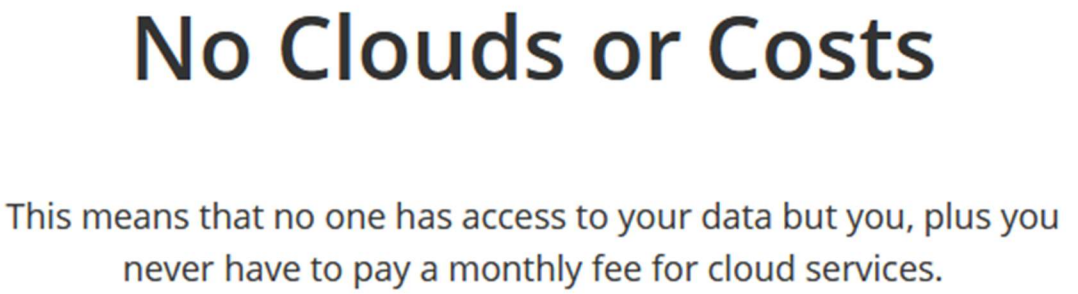
34. Additionally, Anker's privacy policy, which is included on Anker's website, does not disclose that the Camera Products collect and store video and facial recognition information.

35. Accordingly, Defendants represented that images and videos captured by the Camera Products were stored and processed solely on the camera and/or the user's local network, and were not transmitted to Defendants' cloud storage, let alone to cloud storage hosted by a third party. Defendants further represented that facial recognition was performed locally and that biometric information was not shared with anyone, and that strong encryption was used for all data captured by the Camera Products.

36. In addition, as noted above, Defendants offer the eufy Security App for use with the Camera Products. Defendants offer this app to consumers via the Google Play store, where Defendants represent that "[n]o data [is] shared with third parties" and that the app *may* collect only one type of personal info (*i.e.*, an email address). Defendants make equivalent

representations in connection with offering the eufy Security App to consumers via Apple's App Store.

37. Finally, the "Anker Privacy Policy" available to consumers does not disclose that Defendants will collect, transmit, and disseminate images and biometric information (*i.e.*, face templates) to third parties, including when the user has not created a cloud account or consented to such use of their images and information. Instead, it claims that eufy cameras operate with "[n]o [c]louds" and that "no has access to your data but you," as follows:



C. Purchasers of the Camera Products Rely On Defendants' Misrepresentations

38. Many users, including Plaintiffs, selected the Camera Products in reasonable reliance on Defendants' representations concerning privacy and security and would not have purchased the products, or would have paid less for them, had Defendants truthfully represented their privacy and security practices. Defendants knew that consumers relied on their statements concerning the privacy and security features of the Camera Products, and Defendants designed and conducted a long-term marketing campaign touting these features to attractive privacy-conscious consumers.

39. The data wrongfully collected, transmitted, and disseminated by Defendants includes "biometrics," or "biometric information." "Biometrics" refers to unique physical

characteristics used to identify an individual. One of the most prevalent uses of biometrics is in facial recognition technology, which works by scanning a human face or an image thereof, extracting facial feature data based on specific biometric identifiers, and comparing the resulting "face template" (or "faceprint") against templates stored in a database. If a match is found, an individual may be identified.

40. Facial recognition technology in consumer products presents substantial consumer privacy concerns. For instance, an individual's face template may be used as a password enabling the individual to access an app or program, or a device such as a cellular phone. Critically, while a password may be changed by the consumer if it is subject to a data breach, a face template *cannot* be changed. Thus, maintaining biometric information securely is especially important for consumers. For that reason, the Federal Trade Commission ("FTC") has emphasized that companies should obtain affirmative consent from consumers before collecting biometric identifiers and information from digital photographs and videos.

D. Security Professionals Find That Anker's Representations Are False

41. While consumers, including Plaintiffs, reasonably believed Anker's representations concerning privacy and security, it was not until November 2022 that consumers discovered the data associated with their Camera Products was being sent to Anker and was not protected using Military-Grade AES-256 data encryption.

42. On Thanksgiving Day 2022, Security researcher Paul Moore posted a string of tweets and videos, demonstrating that the Camera Products were uploading name-tagged thumbnail images to Anker's AWS-hosted cloud storage, without encryption. Put differently, Anker was accessing and storing the notification that the Camera Products send to customers' smart phones and other devices. Even worse, a very weak AES key was being used to encrypt

video footage, which could be easily brute forced.[2] This was not "Military-Grade AES-256 data encryption."

43. On November 23, 2022, Moore uploaded a video that demonstrated his findings. With his eufy Homebase unplugged, Moore walked in front of his camera. From an incognito web browser, Moore could pull up a thumbnail image of himself, an image of the feed shortly before he was visible, and—perhaps more concerning—ID numbers indicating his recognized face and his status as the camera owner.[3] In other words, the Camera Products paired consumers' facial scans with other personally identifiable information from the consumer, which made Defendants capable of determining consumers' identities. This further suggests that all this information had been uploaded to a web server.

44. Moore's findings were confirmed by others. One day later, security firm SEC Consult summarized two years of analyzing a eufyCam, noting a similar transfer of thumbnails through a cloud service. The company also saw the weak keys, suggesting "hard-coded encryption/decryption keys which are identical for all sold Homebase devices," though it was unclear for what the keys were being used.[4] Additionally, media outlets seemed to be able to replicate the same results.[5]

45. Indeed, U.S.-based online technology media outlet *The Verge* was able to stream video from Anker's Camera Products, because the stream was not encrypted. The report noted that, "[t]his week, we repeatedly watched live footage from two of our own eufy cameras using that very same VLC media player, from across the United States—proving that

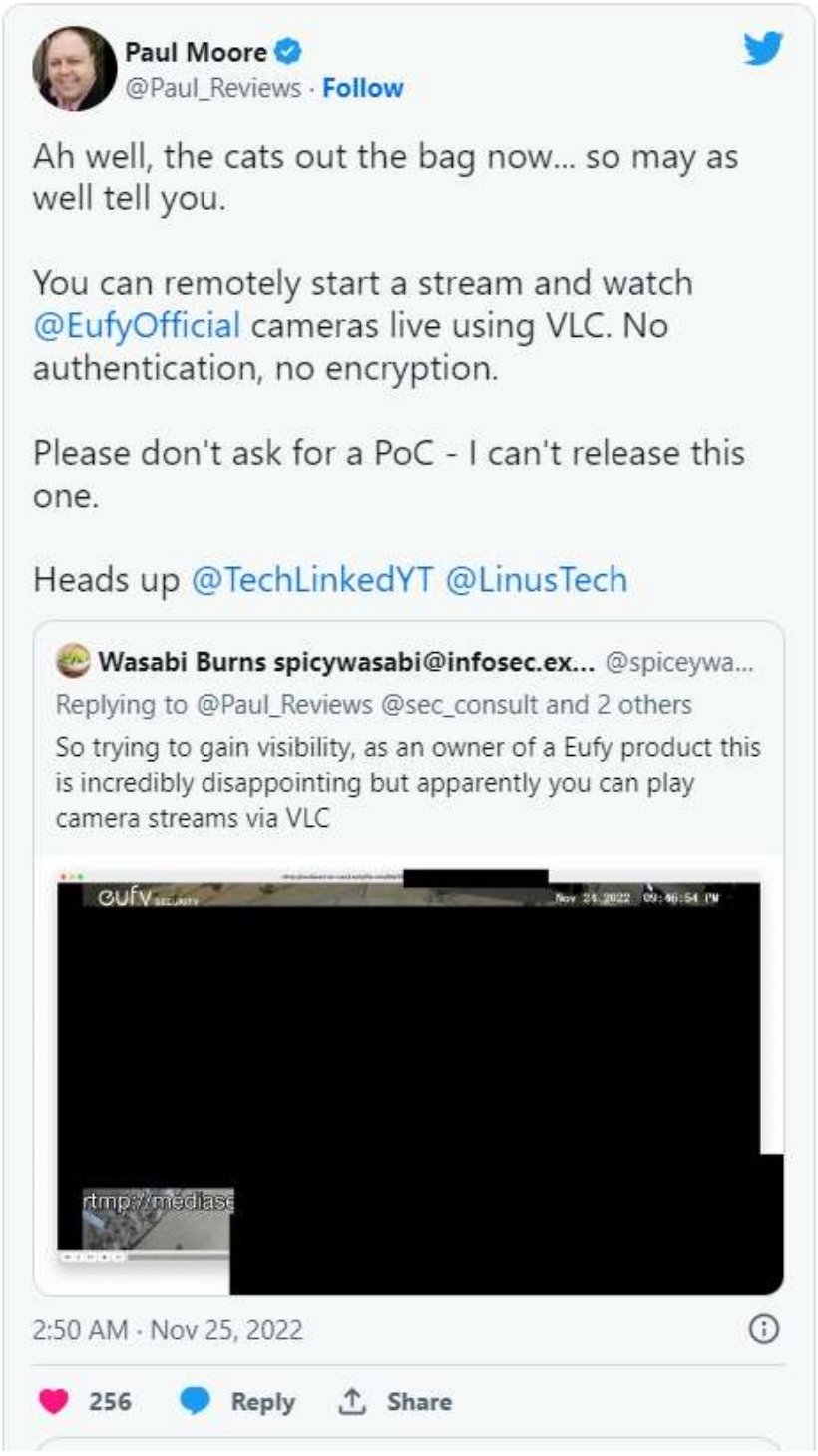
[2] *See* https://twitter.com/Paul_Reviews/status/1594725532062580737;
[3] *See* https://www.youtube.com/watch?v=qOjiCbxP5Lc.
[4] *See* https://sec-consult.com/blog/detail/the-eufycam-long-term-observation/.
[5] *See* https://www.theverge.com/2022/11/30/23486753/anker-eufy-security-camera-cloud-private-encryption-authentication-storage.

Anker has a way to bypass encryption and access these supposedly secure cameras through the cloud."[6]

46. Although it was obvious that Defendants' statements about the Camera Products' security features were false, Defendants refused to admit the truth. On November 30, 2022, Sean Hollister of *The Verge* wrote that he "asked Anker point-blank to confirm or deny" whether the Company's Camera Products streamed video without encryption and Defendants categorically denied it: "I can confirm that it is not possible to start a stream and watch live footage using a third-party player such as VLC," Brett White, a senior PR manager at Anker, told Hollister via email.

47. Indeed, another user, posting under the name "Wasabi Burns," tweeted that he was able to play eufy camera streams using the VLC player.

[6] *Id.*



48. Moore, The Verge, and Wasabi Burns showed that Anker's claim that footage was "sent straight to your phone—and only you have the key" was patently false. Accordingly, Anker's advertisements and warranties that all camera data was stored locally,

that Anker and others could not access the information, and that all information was encrypted were untrue, rendering Anker's Camera Products less valuable than a camera system that did have such security and privacy futures.

E. Anker Unlawfully Collects Facial Recognition Information

49. Anker's actions do not only represent a serious breach of confidence, but also an illegal misappropriation of biometric data.

50. Biometric Data is particularly sensitive personal information. As the Illinois Legislature has found, "[b]iometrics are unlike other unique identifiers that are used to access finances or other sensitive information." 740 ILCS 14/5(c). "For example, social security numbers, when compromised, can be changed. Biometrics, however, are biologically unique to the individual; therefore, once compromised, the individual has no recourse, is at heightened risk for identity theft, and is likely to withdraw from biometric-facilitated transactions." *Id.*

51. In recognition of these concerns over the security of individuals' Biometric Data, the Illinois Legislature enacted Biometric Information Privacy Act ("BIPA"), which provides, *inter alia*, that a private entity may not obtain and/or possess an individual's Biometric Data unless it: (1) informs that person (or their representative) in writing that a biometric identifier or biometric information is being collected or stored, *id.* 14/15(b)(1); (2) informs that person in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used, *id.* 14/15(b)(2); (3) receives a written release from the person (or their representative) for the collection of his or her biometric identifier or information, *id*. 14/15(b)(3); and (4) publishes publicly available

written retention schedules and guidelines for permanently destroying Biometric Data, *id.* 740 ILCS 14/15(a).

52. Further, the entity must store, transmit, and protect from disclosure all Biometric Data using the same standard of care in the industry and in a manner at least as protective as the means used to protect other confidential and sensitive information. *Id.* 14/15(e).

53. In direct violation of each of the foregoing provisions of BIPA, Anker collected and captured facial recognition information from Plaintiffs and Class members, as well as their friends and family that appear on their cameras. This information was then uploaded to Anker's servers, and stored there, without notice, prior consent, or providing a publicly available policy establishing a retention schedule and guidelines for permanently destroying this Biometric Data. And as explained herein, the products paired consumers' facial scans with other personally identifiable information from the consumer, which made Defendants capable of determining consumers' identities. Additionally, Anker's methods for securing such information was woefully inadequate. Consequently, Anker violated BIPA.

F. Defendants Knew That the Camera Products Transmitted Images and Biometric Information to Cloud Storage

54. During the relevant time period, Defendants were aware that they were misleading consumers. Defendants specifically designed the Camera Products to communicate consumer data, over the internet, without military-grade encryption, often to Defendants' own servers. Despite Defendants' exclusive knowledge regarding the design and operation of their Camera Products, Defendants still made the false privacy claims alleged herein. But it was not until third-party security experts examined the Camera Products, and published their results, that Defendants were forced to address their misstatements.

55. Defendants eventually admitted that they were already aware that their eufy cameras transmitted images and biometric information to their AWS-hosted cloud storage. In an email to Moore, a eufy "Customer Service Engineer specialized in safety and privacy" wrote that "the app needs to communicate with the cloud server *in real-time*" (emphasis added) (referring to the transmittal of images to Defendants' cloud storage and the application of facial recognition technology to such images on the cloud) and wrote that "we have also noticed it before," stating that Defendants were already developing a new-generation product that would function differently.

56. On November 29, 2022, after technology security researchers drew public attention to Defendants' misrepresented practices, Defendants issued a public statement conceding that they had misled consumers. Specifically, Defendants conceded that thumbnails (or preview images) of videos are transmitted to and hosted on a cloud server maintained by a third party, namely AWS.

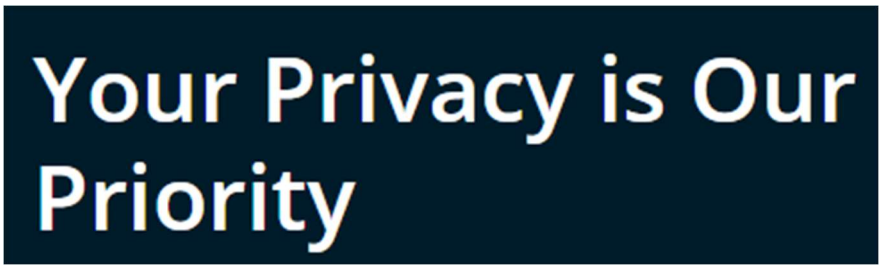
57. Defendants stated:

> Although our eufy Security app allows users to choose between text-based or thumbnail-based push notifications, it was not made clear that choosing thumbnail-based notifications would require preview images to be briefly hosted in the cloud.
>
> That lack of communication was an oversight on our part and we sincerely apologize for the error.

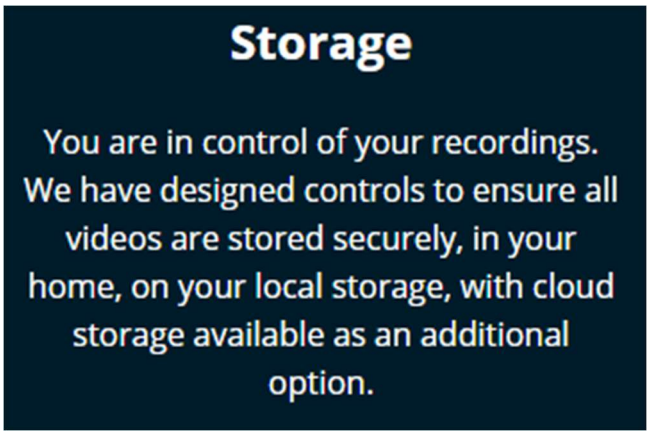
58. Furthermore, Defendants stated that they were "revising the push notifications language in the eufy Security app to clearly detail that push notification with thumbnails require preview images that will be temporarily stored in the cloud," and that they "will be more clear about the use of cloud for push notifications in our consumer-facing marketing materials."

59. Defendants, however, have failed to fulfill these promises. As of December 20, 2022, Defendants' eufy website for US consumers (us.eufy.com) continued to state "No Clouds or Costs" for the eufy Video Doorbell Dual camera, falsely representing that the product did not collect and transmit images to Defendants' cloud storage. According to Defendants, "[t]his means that no one has access to your data but you."

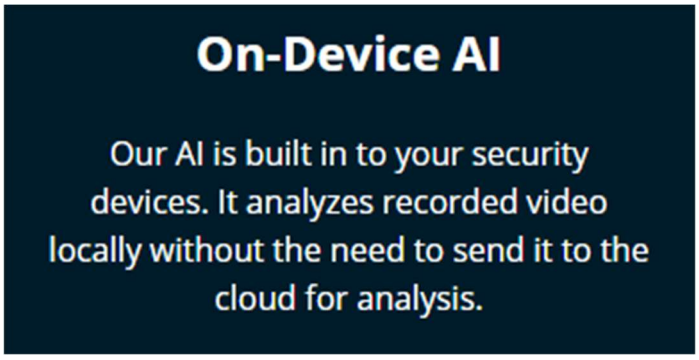
60. Furthermore, Defendants' "Privacy Commitment" page on the eufy website for US consumers continues to misleadingly represent Defendants' privacy practices, reassuring consumers that consumer privacy is Defendants' priority:



61. Defendants also continue to represent that "all videos are stored securely, in your home, on your local storage, with cloud storage available as an additional option," misleadingly omitting that images and biometric information are transmitted to Defendants' cloud storage without users' knowledge or consent, even for users that did not create an account for Defendants' cloud storage, as follows:



62. Furthermore, Defendants emphasize that artificial intelligence features of eufy cameras are built into the devices, misleadingly omitting that it applies facial recognition technology to images and biometric information transmitted, without users' knowledge or consent, to cloud storage hosted by AWS, claiming:



63. Thus, Defendants continued to mislead consumers and users of eufy cameras, and injunctive relief is appropriate.

G. Defendants Belatedly Claim to Have Resolved the Privacy Weaknesses Plaguing the Camera Products

64. On January 31, 2023, *The Verge* published an article describing how "[i]n a series of emails to *The Verge*, Anker has finally admitted its eufy security cameras are not natively end-to-end encrypted — they can and did produce unencrypted video streams for eufy's web portal, like the ones we accessed from across the United States using an ordinary media player."

65. Among other things, Eric Villines, Anker's global head of communications, admitted that prior denials from Defendants to *The Verge* that the Camera Products produced unencrypted video streams had been inaccurate, stating that "Concerning the PR representative who answered your question about using VLC, they conflated the question. This was a known issue, easily replicated and had been reported by the media."

66. This, too, was only admitted after "[The Verge] gave [Anker] an ultimatum: if Anker wouldn't answer why it's supposedly always-encrypted Eufy cameras were producing unencrypted streams—among other questions—we would publish a story about the company's lack of answers."

67. Defendants also assured *The Verge* that Anker's Camera Products now, finally, had end-to-end encryption for "all videos (live and recorded) shared between the user's device to the eufy Security Web portal or the eufy Security App . . . implemented using AES and RSA algorithms."

TOLLING ALLEGATIONS

68. Any applicable statute of limitations should be tolled by the Discovery Rule. Here, Plaintiffs and other Class members reasonably relied on Anker's representations regarding the fact that its Camera Products store all information locally, do not share such information with Anker, and was encrypted.

69. However, it was only on November 21, 2022, when security consultants voiced their concerns that the Camera Products were uploading data to Anker's servers and that the video feeds on these devices were not encrypted that Plaintiffs and other Class members discovered that such representations were false. Consumers exercising reasonable diligence could not have discovered earlier the false and misleading nature of Anker's representations.

70. Accordingly, the Statute of Limitations for all claims, for each Class member, should be tolled until at least November 21, 2022.

CLASS ACTION ALLEGATIONS

71. Plaintiffs bring this action individually and as representatives of all those similarly situated pursuant to Rule 23 of the Federal Rules of Civil Procedure, on behalf of the below-defined classes:

> **National Class:** All persons in the United States who purchased the Camera Products for personal or household use, and not for resale, during the applicable statute of limitations.
>
> **Illinois Class:** All persons in the State of Illinois who purchased the Camera Products during the applicable statute of limitations.
>
> **New York Class:** All persons in New York State who purchased the Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period.
>
> **Florida Class:** All persons in Florida who purchased the Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period.
>
> **Massachusetts Class:** All persons in Massachusetts who purchased the Camera Products for personal or household use, and not for resale, during the applicable statute of limitations period.

The following are excluded from the classes: (1) government entities; (2) any Judge presiding over this action and members of his or her family; (3) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which a Defendant or its parent has a controlling interest (as well as current or former employees, officers, and directors); (4) persons who properly execute and file a timely request for exclusion from the Class; (5) persons whose claims in this matter have been finally adjudicated on the merits or otherwise released; (6) Plaintiffs' counsel and Defendants' counsel; and (7) the legal representatives, successors, and assigns of any such excluded persons.

72. The classes described in this complaint may be jointly referred to as the "Class" or "Classes" and members of the proposed classes may be jointly referred to as "Class

members." Plaintiffs reserve the right to amend or modify the Class definitions with greater specificity, further division into subclasses, or with limitation to particular issues as discovery and the orders of this Court warrant. In addition, the Court can define the Classes and create additional subclasses as may be necessary or desirable to adjudicate common issues and claims of the Class members if, based on discovery of additional facts, the need arises.

73. Pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure, Defendants have acted or refused to act on grounds generally applicable to the Classes, thereby making final injunctive relief or corresponding declaratory relief and damages appropriate with respect to the Classes as a whole. Defendants continue to falsely market eufy cameras as operating with "no clouds," continue to misrepresent that they apply facial recognition technology to images captured by eufy cameras, and continue to apply facial recognition technology to images captured by eufy cameras without users' knowledge or consent.

74. Certification of Plaintiffs' claims for class-wide treatment is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions alleging the same claims.

75. The members of the Class are so numerous that individual joinder of all Class members is impracticable. On information and belief, Class members number in the thousands. The precise number or identification of members of the Class is presently unknown to Plaintiffs, but may be ascertained from Defendants' books and records. Class members may be notified of the pendency of this action by recognized, Court-approved notice dissemination methods, which may include U.S. mail, electronic mail, Internet postings, and/or published notice.

76. Common questions of law and fact exist as to all members of the Class, which predominate over any questions affecting individual members of the Class. These common questions of law or fact include, but are not limited to, the following:

a) Whether the marketing, advertising, packaging, labeling, and other promotional materials for the Camera Products was deceptive;

b) Whether Anker's actions violate the consumer protection statutes invoked herein;

c) Whether Anker unlawfully collected, transmitted, and disseminated images and biometric information from Plaintiffs and Class members' Camera Products;

d) Whether Anker disclosed to Plaintiffs and Class members before they purchased Camera Products that images and biometric information from such cameras would be collected and transmitted by Anker;

e) Whether Anker omitted material facts with regard to the collection and transmittal of images and biometric information from the Camera Products;

f) Whether Plaintiffs and Class members consented to the collection and transmittal of images and biometric information from the Camera Products;

g) Whether Anker's marketing of their camera products was likely to deceive or mislead reasonable consumers;

h) Whether Anker's conduct constitutes violations of the laws and statutes asserted herein;

i) Whether Anker warranted that data collected by the Camera Products would be stored locally and would be encrypted;

j) Whether Anker's conduct was knowing and/or negligent;

k) Whether Defendants were unjustly enriched at the expense of Plaintiffs and Class members;

l) Whether Plaintiffs and Class members are entitled to damages, including compensatory, exemplary, and statutory damages, and the amount of such damages;

m) Whether Plaintiffs and the other Class members have been injured and the proper measure of their losses as a result of those injuries;

n) Whether Plaintiffs and the Class members are entitled to injunctive, declaratory, or other equitable relief; and

o) Whether, as a result of Anker's conduct, Plaintiffs and Class members are entitled to an award of reasonable attorneys' fees, prejudgment interest, or costs of suit.

77. Anker engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs, on behalf of themselves and the other Class members. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quality and quantity, to the numerous common questions that dominate this action.

78. Plaintiffs' claims are typical of the claims of the other Class members because, among other things, all such claims arise out of the same wrongful course of conduct engaged in by Anker in violation of law as complained of herein. Further, the damages of each Class member were caused directly by Anker's wrongful conduct in violation of the law as alleged herein.

79. Plaintiffs are adequate representatives of the Class because they are members of the Class and their interests do not conflict with the interests of the Class members that they seek to represent. Plaintiffs have also retained counsel competent and experienced in complex commercial and class action litigation. Plaintiffs and their counsel intend to prosecute this action vigorously for the benefit of all Class members. Accordingly, the interests of the Class members will be fairly and adequately protected by Plaintiffs and their counsel.

80. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this class action. The damages or other financial detriment suffered by Plaintiffs and the Class members are relatively small compared to the burden and expense that would be required to individually litigate their claims against Anker, so it would be

impracticable for Class members to individually seek redress for Anker's wrongful conduct. Even if Class members could afford individual litigation, the court system could not. Individualized litigation creates a potential for inconsistent or contradictory judgments and increases the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties, and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I

Violation Of The Illinois Consumer Fraud and Deceptive Trade Practices Act ("ICFA")
815 ILCS 505/1, *et seq.*
(On Behalf of Plaintiffs and the National Class and, alternatively, the Illinois Class)

81. Plaintiffs re-allege and incorporate the allegations above as if set forth herein.

82. Illinois law applies under the terms of the EULA.

83. Plaintiffs and other Class members are persons within the context of the ICFA, 815 ILCS 505/1(c).

84. Anker is a person within the context of the ICFA, 815 ILCS 505/1(c).

85. At all times relevant hereto, Anker was engaged in trade or commerce as defined under the ICFA, 815 ILCS 505/1(f). 183.

86. Plaintiffs and the proposed Class are "consumers" who purchased the Products for personal, family, or household use within the meaning of the ICFA, 815 ILCS 505/1(e).

87. The ICFA prohibits engaging in any "unfair or deceptive acts or practices … in the conduct of any trade or commerce…." ICFA, 815 ILCS 505/2.

88. The ICFA prohibits any deceptive, unlawful, unfair, or fraudulent business acts or practices including using deception, fraud, false pretenses, false promises, false advertising, misrepresentation, or the concealment, suppression, or omission of any material

fact, or the use or employment of any practice described in Section 2 of the Uniform Deceptive Trade Practices Act ("UDTPA"). 815 ILCS § 505/2. Plaintiffs and the other Class members reasonably relied upon Anker's representation that the Camera Products stored all data locally and encrypted such data.

89. Anker's conduct, as described herein, constitute unfair or deceptive acts or practices in the course of trade and commerce, in violation of 815 ICFA 505/1, *et seq*.

90. Anker violated the ICFA by representing that the Camera Products have characteristics or benefits that they do not have. 815 ILCS § 505/2; 815 ILCS § 510/2(7).

91. Anker advertised the Camera Products with intent not to sell them as advertised, in violation of 815 ILCS § 505/2 and 815 ILCS § 510/2(9).

92. Anker engaged in fraudulent and/or deceptive conduct, which creates a likelihood of confusion or of misunderstanding in violation of 815 ILCS § 505/2; 815 ILCS § 510/2(3).

93. Anker engaged in misleading and deceptive advertising that represented that the Camera Products stored all data locally and encrypted such data. Anker chose to advertise and label the Camera Products in this way to impact consumer choices and gain market dominance, as it is aware that all consumers who purchased the Camera Products were exposed to and would be impacted by its misrepresentation and would reasonably believe that the Camera Products stored all data locally and encrypted such data. However, the Camera Products do not store all data locally and encrypted such data, which has been demonstrated by security experts and the media.

94. Anker intended that Plaintiffs and each of the other Class members would reasonably rely upon their misrepresentations, characterizations, warranties, and material misrepresentations concerning the true nature of the Camera Products.

95. Anker's misrepresentations, concealment, omissions and other deceptive conduct were likely to deceive and cause misunderstanding and/or in fact caused Plaintiffs and each of the other Class members to be deceived about the true nature of the Camera Products.

96. Plaintiffs and Class members have been damaged as a proximate result of Anker's violations of the ICFA and have suffered damages as a direct and proximate result of purchasing the Camera Products.

97. As a direct and proximate result of Anker's violations of the ICFA, as set forth above, Plaintiffs and the Class members have suffered ascertainable loss of money caused by Anker's misrepresentations.

98. Had they been aware of the true nature of the Camera Products, Plaintiffs and Class members either would have paid less for the Products or would not have purchased them at all.

99. Plaintiffs and the Class members are therefore entitled to relief, including restitution, actual damages, treble damages, punitive damages, costs and attorney's fees, under sections 815 ILCS 505/10a of the ICFA. Plaintiffs and Class members are also entitled to injunctive relief, seeking an order enjoining Anker's unfair and/or deceptive acts or practices.

COUNT II

Violation of New York Deceptive Acts and Practices Law
(New York General Business Law §§ 349 and 350)
(On Behalf of Plaintiffs Bleiberg and Rothberger and the New York Class)

100. Plaintiffs re-allege and incorporate the allegations contained in paragraphs 1–99 above as if fully set forth herein.

101. By the acts and conduct alleged herein, Anker committed deceptive acts and practices in the State of New York by making the above alleged misrepresentations directed to consumers in New York.

102. Plaintiffs and other members of the New York Class are "consumers" in accordance with New York General Business Law ("GBL") § 349.

103. Anker's statements concerning the security and privacy of the Camera Products, alleged above, were advertisements in accordance with GBL § 350.

104. Anker's statements concerning the security and privacy of the Camera Products, alleged above, were misleading in violation of GBL §§ 349 and 350.

105. At all relevant times, Anker conducted trade and commerce in New York and elsewhere within the meaning of GBL § 349, and profited from the sale of the Camera Products within New York.

106. Section 349 allows a plaintiff to recover "actual damages or fifty dollars, whichever is greater." N.Y. Gen. Bus. L. §349(h). Section 350 allows a plaintiff to recover "actual damages or five hundred dollars, whichever is greater." *Id.* §350-e.

107. As a direct and proximate result of Anker's conduct, Plaintiffs and other members of the Class have suffered damages.

108. Accordingly, Plaintiffs and the Class seek to enjoin the unlawful acts and practices described herein, to recover actual damages or statutory damages of fifty dollars and

five hundred dollars under GBL §§ 349 and 350, respectively, whichever is greater, as well punitive damages and reasonable attorneys' fees and costs.

COUNT III

Violation of the Federal Wiretap Act
8 U.S.C. §§ 2510, *et seq.*
(On Behalf of the National Class)

109. Plaintiffs re-allege and incorporate the allegations contained in paragraphs 1–99 above as if fully set forth herein.

110. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communication through the use of a device. 18 U.S.C. § 2511.

111. The Wiretap Act protects both the sending and receipt of communications.

112. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

113. As set forth above, Anker represents, through its advertising, labeling, marketing, and packaging, that the Camera Products stored all data locally and encrypted such data. However, when electronic notifications are sent between the Camera Products and the user's device (such as a notification that activity has been spotted on the camera), such communications are contemporaneously intercepted and sent to Anker's server.

114. The communications intercepted by Anker included "contents" of electronic communications made between the Camera Products and Plaintiffs and other Class members, such as the image associated with the notification and any facial recognition information.

115. The transmission of data between the Class members' smart phones and their Camera Products were "transfer[s] of signs, signals, writing, . . . data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetic,

photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12). The Camera Products, Class members' smart phones, Anker's server, and the code used by Anker to direct communications to their servers are "devices" within the meaning of 18 U.S.C. § 2510(5).

116. Anker was not an authorized party to the communication because the Plaintiffs and Class members were unaware of Anker's redirecting of the camera notification to its own server. Class members did not consent to Anker's interception of their camera notification.

117. After intercepting the communications, Anker then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(1)(a).

118. As a result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs and the Class members, injunctive and declaratory relief, punitive damages, and reasonable attorneys' fee and other litigation costs.

COUNT IV

Violation Of Biometric Information Privacy Act ("BIPA")
740 ILCS 14/1, *et seq.*
(On Behalf of Plaintiffs and National Class and, alternatively, the Illinois Class)

119. Plaintiffs re-allege and incorporate the contained in paragraphs 1–99 above as if fully set forth herein.

120. Illinois law applies under the terms of the EULA.

121. BIPA makes it unlawful for any private entity to, among other things, "collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifiers or biometric information, unless it first: (1) informs the subject . . . in

writing that a biometric identifier or biometric information is being collected or stored; (2) informs the subject . . . in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and (3) receives a written release executed by the subject of the biometric identifier or biometric information . . . .” 740 ILCS 14/15(b).

122. Anker is a corporation and Fantasia and Power Mobile are limited liability companies and thus each entity qualifies as a “private entity” under BIPA. *See* 740 ILCS 14/10.

123. Plaintiffs and the Class members are individuals who had their biometrics collected and stored by Anker. *See* 740 ILCS 14/10.

124. Prior to collecting and using Plaintiffs’ biometric identifiers, Anker required that each user provide their email address through the eufy Security App. This information enables Defendants to associate the collected biometric identifiers with Plaintiffs’ identities, as evidenced in part by the unique ID numbers and name-tagged thumbnail images uploaded to Anker’s AWS-hosted cloud storage, without encryption.

125. Anker systematically collected, used, and stored Plaintiffs and the Class members’ Biometric Data derived from Plaintiffs and the Class members’ facial geometry without first obtaining the written release required by 740 ILCS 14/15(b)(3), and thereby uniformly invaded Plaintiffs and each Class member’s statutorily protected right to privacy in their biometrics.

126. Anker failed to properly inform Plaintiffs or members of the Class in writing that their Biometric Data was being collected, stored, or otherwise obtained, and of the

specific purpose and length of term for which those biometrics were being collected, stored, and used, as required by 740 ILCS 14/15(b)(1)-(2).

127. In addition, Anker does not provide a written, publicly available retention schedule and guidelines for permanently destroying the Biometric Data of Plaintiffs or the Class members, as required by BIPA. *See* 740 ILCS 14/15(a). Anker's failure to provide such a schedule and guidelines constitutes an independent violation of the statute.

128. Each instance in which Anker collected, stored, used, or otherwise obtained Plaintiffs and/or Class members' Biometric Data, as described herein, constitutes a separate violation of the statutory right of Plaintiffs and each Class member to keep private this Biometric Data, as set forth in BIPA, 740 ILCS 14/1, *et seq*.

129. On behalf of themselves and the Class members, Plaintiffs seek: (1) injunctive and equitable relief as is necessary to protect the interests of Plaintiffs and the Class by requiring Anker to comply with BIPA's requirements, including BIPA's requirements for the collection, storage, and use of biometric identifiers and biometric information as described herein, and for the provision of the requisite written disclosure to consumers; (2) statutory damages of $5,000.00 for each and every intentional and reckless violation of BIPA pursuant to 740 ILCS 14/20(2), or, alternatively, statutory damages of $1,000.00 for each and every violation pursuant to 740 ILCS 14/20(1) if the violations are found to have been committed negligently; and (3) reasonable attorneys' fees and costs and other litigation expenses pursuant to 740 ILCS 14/20(3).

COUNT V

Violation of Mass. G. L. 93A
(On Behalf of Plaintiff Farr and the Massachusetts Class against All Defendants)

130. Plaintiff Farr re-alleges and incorporates the allegations contained in paragraphs 1- 99, above as if fully set forth herein.

131. Plaintiff Farr and Defendants are each "persons" as defined by Mass. G.L. 93A, § 1(a).

132. Plaintiff Farr and the Massachusetts Class members are all purchasers of the eufy Camera Products.

133. Defendants engage in "trade" and "commerce" in Massachusetts through the marketing, advertising, distribution, and sale of the eufy Camera Products at issue, as defined by Mass. G.L. 93A, § 1(a).

134. Mass. G.L. 93A § 2 prohibits and declares unlawful "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce" in the Commonwealth of Massachusetts.

135. This Count is brought pursuant to Mass. G.L. 93A, § 9, as Plaintiff Farr and the Proposed Massachusetts Class members are not involved in trade or commerce such that Mass. G.L. 93A, § 11 applies, and have been injured by Defendants' violation of Mass. G.L. 93A § 2.

136. Upon information and belief, Defendants Anker Innovations, Power Mobile, and Fantasia do not maintain a place of business or keep assets within Massachusetts, therefore, pursuant to Mass. G.L. 93A § 9(3), the demand requirements of that same paragraph are not required for this claim.

137. Defendants' foregoing unfair methods of competition and unfair or deceptive acts or practices, including their omissions, were and are committed in their course of trade or commerce, directed at consumers, affect the public interest, and injured Plaintiff Farr and the Massachusetts Class members.

138. In violation of Mass. G.L. 93A § 2, Defendants engaged in unfair methods of competition and unfair or deceptive acts or practices by expressly representing on their website, product packaging, and in marketing materials, that the eufy Camera Products have safety and privacy characteristics that they do not have, including but not limited to, misrepresenting that:

- user's data will only be stored locally;
- user's data "never leaves the safety of your home";
- footage from the eufy Security Cameras only gets transmitted with "end-to-end" military-grade encryption, and that it will only send that footage "straight to your phone; and
- the user's private data will "never leave the safety of your home."

139. Defendants knew that their representations of privacy and security were false but failed to correct these misrepresentations or disclose this information to consumers.

140. Defendants also engaged in unfair and deceptive trade practices that violated Mass. G.L. 93A § 2, by actively concealing and omitting material facts about their eufy Camera Products, including but not limited to the fact that the camera feeds were not encrypted, could be viewed by any third party, and that user's information was being captured and sent to Defendants' cloud server.

141. Defendants knew that such information was material to consumer transactions and consumer's decision to purchase the eufy Camera Products.

142. Defendants' unfair or deceptive acts or practices, including concealing, omitting, or suppressing material facts about the operation of the eufy Camera Products had a tendency or capacity to mislead; tended to create a false impression in consumers; and were likely to, and did in fact, deceive reasonable consumers, including Plaintiff Farr and the Massachusetts Class members, about the security and privacy of the eufy Camera Products as well as the quality and true value of the eufy Camera Products.

143. Defendants intended for Plaintiff Farr and the Massachusetts Class members to rely on their misrepresentations and omissions so that Plaintiff Farr and the Massachusetts Class members would purchase their products.

144. Defendants alone knew about the true state of their security and privacy practices and Defendants also knew that no reasonable consumer would purchase the eufy Camera Products had they known of Defendants' misrepresentations and omissions.

145. Defendants' misrepresentations, failure to disclose, and active concealment of, these features were material to Plaintiff Farr and the Massachusetts Class members. Plaintiff Farr and the Massachusetts Class members believed Defendants would adequately protect their privacy and security. These protections were valuable to them, and the protections formed the basis of their bargain.

146. Defendants' general course of conduct is injurious to the public interest, and such acts are ongoing and/or have a substantial likelihood of being repeated because Defendants have not corrected or rectified all their misrepresentations or omissions and, upon information and belief, continue to collect and send consumers' information to the cloud.

147. Plaintiff Kevin Farr and the Massachusetts Class members have suffered and will continue to suffer irreparable harm if these Defendants continue to engage in such deceptive, unfair, and unreasonable practices.

148. As a result of Defendants' deceptive and unfair acts or practices, including Defendants' misrepresentations and omissions, Plaintiff Farr and the Massachusetts Class members have suffered ascertainable losses and actual damages, which include but are not limited to, the costs they incurred paying for products that were not the ones represented to them. Plaintiff Farr and the Massachusetts Class members paid a premium price for the products because they would have paid substantially less had they known that their camera's footage would not be protected as advertised.

149. As a result of Defendants' willful and knowing conduct, Defendants are liable for up to three times the damages that Plaintiff Farr and Massachusetts Class members incurred. *See* Mass. G.L. 93A.

150. In addition, under Mass. G.L. 93A, Plaintiff Farr and the Massachusetts Class members seek to recover attorneys' fees, and equitable and injunctive relief enjoining further violations of the Mass. G.L. 93A.

COUNT VI

Violation of Florida Deceptive and Unfair Trade Practices Act ("FDUTPA"), Fla. Stat. § 501.201 et seq. (On behalf of Plaintiff Desai and the Florida Class)

151. Plaintiff Desai re-alleges and incorporates the allegations contained in paragraphs 1–99 above as if fully set forth herein.

152. Desai and the Class members are "consumer[s]" engaged in "trade or commerce" within the meaning of FDUTPA. Fla. Stat. § 501.203 (7), (8). Anker engages in "trade or commerce" within the meaning of FDUTPA. Fla. Stat. § 501.203(8).

153. FDUTPA prohibits "[u]nfair methods of competition, unconscionable acts or practices, and unfair or deceptive acts or practices in the conduct of any trade or commerce." Fla. Stat. § 501.204(1).

154. Defendants engaged in unfair and deceptive trade practices that violated FDUTPA, by representing that their security cameras have safety and privacy characteristics that they do not have, including but not limited to the following:

a. Anker misrepresented that user's data will only be stored locally;

b. Anker misrepresented that user's data "never leaves the safety of your home";

c. Anker misrepresented that footage from the eufy Security Cameras only gets transmitted with "end-to-end" military-grade encryption, and that it will only send that footage "straight to your phone; and

d. Anker misrepresented that the user's private data will "never leave the safety of your home."

155. Anker knew that its representations of privacy and security were false but failed to disclose this information to consumers. Anker knew that such information was material to consumer transactions and consumer's decision to purchase the eufy Camera Products.

156. Anker actively concealed and misrepresented the true nature of how their eufy Camera Products operated. Anker intended for Desai and Florida Class members to rely on their misrepresentations and omissions so that Plaintiff and the Florida Class members would purchase their products. Anker's unfair or deceptive acts or practices, including concealing, omitting, of suppressing material facts about the operation of the eufy Camera Products had a tendency or capacity to mislead; tended to create a false impression in consumers; and were likely to, and did in fact, deceive reasonable consumers, including Desai and the Florida Class members, about the security and privacy of the eufy Camera Products as well as the quality and true value of the Products.

157. Anker intentionally and knowingly misrepresented or omitted material facts regarding the eufy Camera Products' security and privacy with an intent to mislead Plaintiff and the Florida Class members.

158. Anker knew or should have known that its conduct violated the FDUTPA.

159. Desai and the Florida Class members were and are injured as a result of Anker's conduct because they paid to own the Camera Products that would protect their information and privacy by only storing the information "locally." Instead, Desai and the Florida Class members received and overpaid for eufy Camera Products that transmitted and stored unencrypted information over the internet.

160. Anker's failure to disclose, and active concealment of, these features were material to Desai and the Florida Class members.

161. Desai and the Florida Class members have suffered ascertainable losses as a result of Anker's misrepresentations and omissions about the eufy Camera Products. Had they been aware of the true nature of how the eufy Camera Products operated, they either would have paid less for the cameras or would not have purchased the cameras. Desai and the Florida Class members did not receive the benefit of their bargain due to Anker's misconduct.

162. As a direct and proximate result of Anker's violations of FDUTPA, Desai and the Florida Class members have suffered injury-in-fact and actual damages.

163. Desai and the Florida Class members are entitled to recover their actual damages under Fla. Stat. § 501.211(2) and attorneys' fees under Fla. Stat. § 501.2105(1).

164. Desai and the Florida Class members have suffered and will continue to suffer irreparable harm if Anker continues to engage in such deceptive, unfair, and unreasonable practices.

165. Desai, on behalf of the Florida Class, requests that the Court award actual damages and injunctive relief enjoining further violations of FDUTPA, as well as award Desai and the Florida Class members' attorneys' fees; and any other just and proper relief available under FDUTPA.

COUNT VII

Unjust Enrichment
(In the Alternative and on Behalf of the National Class and, alternatively, the Illinois Class, the New York Class, the Massachusetts Class, and the Florida Class)

166. Plaintiffs re-allege and incorporate the allegations contained in paragraphs 1–99 above as if fully set forth herein.

167. Plaintiffs and the other members of the Class conferred benefits on Anker by purchasing the Camera Products.

168. Anker has been unjustly enriched in retaining the revenues derived from the purchase of the Products by Plaintiffs and the other members of the Class.

169. Retention of those monies under these circumstances is unjust and inequitable because Anker's labeling of the Products was misleading to consumers, which caused injuries to Plaintiffs and the other members of the Class because they would have not purchased the Camera Products if Anker had disclosed that the Camera Products were not secure.

170. Because Anker's retention of the non-gratuitous benefits conferred on them by Plaintiffs and the other members of the Class is unjust and inequitable, Anker must pay restitution to Plaintiffs and the other members of the Class for their unjust enrichment, as ordered by the Court.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the Class members, prays for judgment and relief against Anker as follows:

a) For an order declaring: (i) this is a class action pursuant to Rule 23 of the Federal Rules of Civil Procedure on behalf of the proposed Class described herein; and (ii) appointing Plaintiffs to serve as representative for the Class and Plaintiffs' counsel to serve as Class Counsel;

b) For an order enjoining Anker from continuing to engage in the unlawful conduct set forth herein;

c) For an order awarding restitution of the monies Anker wrongfully acquired by its illegal and deceptive conduct;

d) For an order requiring disgorgement of the monies Anker wrongfully acquired by its illegal and deceptive conduct;

e) For compensatory and punitive damages, including actual and statutory damages, arising from Anker's wrongful conduct and illegal conduct;

f) For an award of reasonable attorneys' fees and costs and expenses incurred in the course of prosecuting this action; and

g) For such other and further relief as the Court deems just and proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38(b), Plaintiffs demand a trial by jury of all claims in this complaint so triable.

Dated: April 6, 2023

Respectfully submitted,

/s/ Gary M. Klinger

Gary M. Klinger
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
227 W. Monroe Street, Suite 2100
Chicago, Illinois 60606
Telephone: 866.252.0878
gklinger@milberg.com

Attorneys for Plaintiffs and the Putative Classes

CERTIFICATE OF SERVICE

I hereby certify that on this 6th day of April, 2023, I caused a true and correct copy of the foregoing notice to be filed with the Clerk of the Court for the Northern District of Illinois via the Court's CM/ECF system, which will send notification of such filing to the counsel of record in the above-captioned matters.

/s/ Gary M. Klinger
Gary M. Klinger